* Introduction :-

- BPCS (Basic Process control system) :- System responds to input signals From Process, equipment & Programmable sys., operator and generates output signals causing Process To operate but which doesnot Perform any SIF (safety instrumented functions) with SIL ≥ 1 or higher.
  plant normal day
- SIL (Safety integrity level) :- quantifiable measure (low 1 to high 4) of safety system's Performance indicating it's reliability in reducing risk For Critical ind. Proces.
  (4) higher SIL ↑ → Lower Probability of Failure & greater Cost
- DC (Diagnostic Coverage) :- is ratio of detected Failure to total Failure rate
- DCS (Distributed Control System) :- Same as BPCS.
- ESD (Emergency Shut down System) :- logic System designed to execute Safe shutdown action of the plant based on emergency Scenario This is also referred to as SIS.
- SIS (Safety instrumented System) :- a critical, independant automated System That monitors industrial Process and takes actions (like shutdowns) when hazardous Conditions exceed Safe Limits to Prevent accidents,
  → SIS operate Separately From BPCS and designed to Spectific SIL
  → SIS used to implemented one or more Safety instrumented Functions, it's Composed of Sensors, logic Solver and Final elements
- IPL (independent Protection layer) :- have to Potential to Prevent a hazardous event or mitigate The Consequence. " All of IPL are Safeguard but not all Safeguard are IPL) ex. (relief valve, SIS, ...).
- PFD (Probability of Failure on Demand) : average Probability that a System Fails to respond when a demand is placed
- RRF (Risk Reduction Factor) :- inverse PFD ,it's quantifies how much a Safety System to lowers risk

Examples :-

SIL	Safety	PFD	RRF
SIL 4	> 99.99 %	0.001 - 0.01 %	100,000 - 10,000
SIL 3	99.9 - 99.99 %	0.01 - 0.1 %	10,000 - 1000
SIL 2	99 - 99.9 %	0.1 - 1 %	1000 - 100
SIL 1	90 - 99 %	1 - 10 %	100 - 10

CamScanner

- P&ID :Piping & instrumentation digram , PFD:- Process Flow diagram.
- SGS (Safeguarding System.) :- involves servies to manging hazards & risks also called ESD System or logic Solver (ISD, BPCS, Alarm, SIS ESD, PSV, ERP...)
- SFF (Safe Failure Fraction) :- the Fraction of overall random Failure rate of device that results in either a Safe Failure or a dangerous Failure. (Fail Safe = حالة الفشل الآمن , Fail dangerous = حالة الفشل الخطير)
- SIF (Safety instrumented Function) :- Safety Functions with a specified SIL which necessary to achieve Functional Safety, SIF Can be either Protection Function or Control Functions.
- SCE (Safety Critical elements) :- Vital equipment, Systems or structure whose Failure lead to major accident & whose Function to prevent or mitigate high risk ex.. (relief Valves, interlocks, ...)

---

* Hazardous Event :-
  → The release of a material or energy that has the Potential For Causing harmful effects to (plant personal, Surrounding community, environment)
* Risk :-
  → Relates two important factors: → How much damage (Consequence)
  → How often the hazardous event (Likelihood)
* Hazard Identification :-
  → is Fundamental to Safe design & operation ex. (HAZOP, FMEA, Checklist...)
* BLEVE :- Boiling liquid expanding Vapor Explosion
* Fire ball :- spheres of burning flammable gas /vapor after result from BLEVE
* VCE (Vapor cloud explosion.) :- large flammable gas/vapor clouds

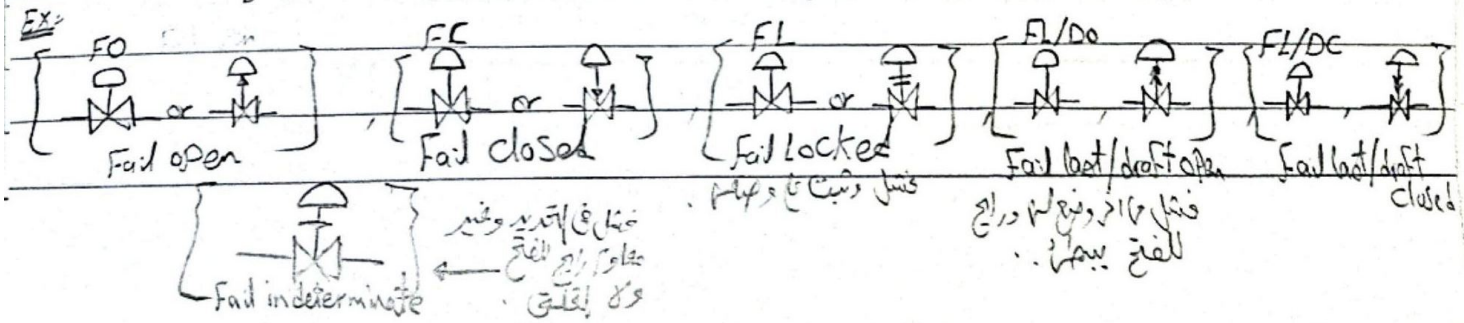
---

* PST (Process Safety time.) :- the Crucial window between Process Failure and hazardous event, define the max time a Safety Sys. act to bring Process to Safe State, ensuring SIF respond Fast enough to prevent Catastrophic

* Double (or multiple) Jeopardy → (unrelated or unlinked)
  - two independent, unlikely failures occurring simultaneously.
  - The chance that two (or more) unrelated events or incident will occur at some time
  - If two (or more) events or incident arising from a common cause it's called common cause and do not qualify double jeopardy.
  → Double (or more) Jeopardy
* Common Cause Failure (CCF) → (linked)
  - failure are dependent linked by single cause
  - used in HAZOP / PHA
  - events have something in common
* Simultaneous Failure - (the umbrella term)
  - Multiple components failing at once due to one shared failure cause including (dependence or independence).
  - in it the second failure occure while the first is still active

---

* Fail Safe :-
  - If failure of a component, signal or utility action that return the system to a safe condition.
  - Design features which provide for the maintenance of safe operating conditions in the event of a malfunction of control devices or an interruption of an energy source
* Fail dangerous :-
  - if failure cause catastrophic or hazardous events.



* PHA :-

- is a systematic multidisciplinary team study
- it focuses on identifying & analyzing the significance of potential process hazards and make initial recommendations for eleminate and/or reducing the consequences.
- it's the foundation of any process safety managment.
- it's interested in potential causes, likelihood & consequences.
- it's works by combining experience & knowledge of expert teams with a selected analytical methodology
- it's provides companies with info to make operating decisions to help improve safety & manage risk of operations.
- Various hazard ident. methodologies.
- * it's should be conducted several times during a facility's design, construction and operating life cycle.
- Some methodologies not only identify hazards but also operability problems.
- PHA assigns qualitative likelihood and severity ratings from which a relative risk ranking can be estimated
- PHA identifies high level hazards for possible further quantitative risk analysis

UK at ICT ... 30 ... PHA ...

* Process Safety management :-

* Process Hazard analysis :-
- PHA is about applying the basic Principles of Probability and risk managment to make long term value added decisions.

* Risk Based Decision Process :- (RBDM) Making
- is Choosing the best of a number of alternative to maximize the resources available & minimize the risks.
- The Value to risk-based decisions occur not when you have Complete Control & Knowledge of the future Prospects but When you don't.

1- Group Can lose focus & needs to be re-focused
2- Opinions diverge & converge

* Quantitative & Qualitative Hazard Analysis :-
- Both of Quantitative & Qualitative hazard analysis are important in identifying & analyzing risk.

* PHA	* Risk analysis
- Initial Predictive identification of all potential hazards, estimates likelihood & severity Suggests improvements.	- Subsequent assessent of major hazards only statistically based Probability / Consequence hazard assessment
- Use on every Project at every Stage From Concept Through decommissioning	- Selective, if the Potential exists for Catastrophic accidiat or if no easy solution to identified hazard is evident
- Qualitative, based on experience, Knowledge & Creative thinking of team	- Quantitative, requires extensive (very costly) statistical data & specialized expertise
- Multidisciplinary team	- one or two specally trained people

* Hazards identification & Assessment :-
  - identifies wide range of hazards. & high risk hazards
  - " actual & hidden Potential hazards.
  - Allows hazards to be Prioritized.
  - Provide recommendations for mitigating consequences
  - highlights opportunities for improving operability.

* Hazard Controls :-
  - Design layout information can identify design errors and highlight opportunities for debottlenecting & improving operability.
  - Identifies a need for formal operating, maintenance and emergency Procedures.
  - highlights Weaknesses in existing Procedures
  - Can be adopted to perform Job hazard assessments and Critical task analysis.
  - Identifies the need for a refresher training schedule

* Hazardous Materials :-
  - Identifies → Potential immediate and long term health concerns.
    → " chemical interaction hazards
    → gaps in existing Precautionary Procedures.
  - Can Provide recommendations for mitigating Consequences.

* COSHH :- (Control of Substance Hazard to Health)
  (Hazard materials) التعامل مع المواد الخطرة
  MSDS او ورقة بيانات السلامة

* Elements of Facility Risk :-

⇒ Initiating events :-

- Are the first events in an accident sequence.
- The event or action that sets off a chain reaction.

⇒ Propagating events :-

- Are the secondary events that link an initiating event to an accident outcomes.

---

* Process risk reduction strategies :-

- operator control systems (Alarm, DCS, ESD, F&G.)
- Mitigation Systems (PSV, Bund, Dike, Flare.)
- Procedure
- Emergency plans.
- Training Systems.
- Management.
- Design.

---

* Human Factors in Facility Risk :-

- PHA objective in considering human factor in facility risk.

⇒ Human error is either Active or Latent (waiting to happen) error.

① Active human error :-

- has immediate & direct effect or direct initiator of an chain of events lead to accident

② Latent human error :-

- In it the consequences of error may only become dynamic after a period of time when the condition caused by the original error combines with other errors to bring unsafe cond.

---

* PHA Teams :-
  - At least one member have knowledge to the Process.
  - " " " " " in PHA methodology & evaluation
  - As Few as 2 or 3 & as many 7 or 8 depend on methodology and Complexity, Too many Participants reduce the efficiency of PHA.

⇒ Advantages of team :-
  - wide info, Range of experiences
  - Representative from different (Cultural groups)
  - Groups Can make higher quality decisions

⇒ Disadvantages of team :-
  - Time Pressure - Social Pressure - Ego Pressure.

* Thinking Modes :-
  - Just Facts - Worst Case - Possible Scenario.
  - Big Picture

* General PHA Procedure Flow Chart :-
  1- Define Node or System.
  2- Hazard identification
  3- Possible Hazard Consequence
  4- Identify Existing Safeguards.
  5- Risk Ranking
  6- Recommendation

* يفضل عمل (RaHaZaP) لأن خمس سنوات وهي بتشتغل الأنظمة الحالية.
  - Historical records - operational history.
  - upset & down history - Accident & incident records

* PHA: to identify hazards not to necessarily provide solns to hazards

* PHA study required information. (Process Safety info. PSI)
  - P&ID (Piping & instrument diagram)
  - PFD (Process flow diagram.)
  - MSDS
  - Process flow sheets
  - Process description.
  - ESD Logic
  - Operating & maintenance Procedure.
  - ERPs emergency response plans
  - List of SCE
  - Plot Plans.
  - SLD (single line diagram)
  - Area classification
  - Flare Net...
  - F&G
  - equipment history.

* How identify hazards ?
  - identify Potential loss of Containment Situations.
  - " Causes that result in loss of Containment
  - " Potential Consequences of loss " "
  - " " Safeguards that Prevent or mitigate Consequences. then take actions.

* Methodologies to identify hazards.
  - Preliminary Hazard analysis (PreHA)
  - Hazard and operability Analysis (HAZOP).
  - Failure Mode and effect analysis (FMEA)
  - what if
  - Check list
  - what if & Check list

* PHA :- Process experience is a must.

* Risk analysis:- Quantitative (Ex. FTA, ETA, QRA, LOPA.)
* Hazard identification :- HAZOP, HAZID, FMEA, What if, Check list
* Risk assessment :- May be Qualitative or Quantitative.
* HAZOP, PHA :- Qualitative.

* HAZOP :-

- is the most comprehensive PHA at all stages from design, constran,...
- is group of technique to identifying hazards
- is highly structure hazards identification tools
- best used as late as possible with new design, but for existing facility used at any time.
- makes practically no assumptions

⇒ in it, the process is first broken down into nodes

* Potential causes of hazards may be :-
  - Equipment failure
  - human error
  - Engineering & administrative controls
  - External events or factors

- HAZOP : Can be made to almost any industry
  - Can be used effect to perform job task analysis & procedure.
  - Can be limited by the assumption process will be operate as it was designed to operate.

Reporting ← execution ← preparation : HAZOP مراحل *

* HAZOP types :-
1. HAZOP For process :- Main Doc. require (P&ID).
2. E-HAZOP (Electrical hazop) :- Main ... (SLD)
3. C-HAZOP (Control sys. of hazop) :- Main ... (Network diagram)
4. human HAZOP (or) HAZOP For procedure ← Job Task, Procedure, SOP

* اثناء تقسيم الدراسة ممكن نستخدم
1. Equipment or 2. Stream
وممكن نعمل MIX بين الاثنين

* People Requirements:-
  - up to 8 (max.) ← team size (5-8). ← too many can slow and reduce study quality.
  - Leader (Ask Q.), Recorder (Record discussion), team members.
  - Team leader & Recorder typically are independent of the plant

* Team leader:-
  → Note HAZOP is a team exercise don't let any body including the leader himself to dominate.

* HAZOP Secretary:-
  - Take notes, Record, Check Progress of Chase action, Produce final report

* Process engineer.
  ⇒ description, design, info of Process

* Mechanical design engineer:-
  ⇒ Specification details, Vendor package, equi. & Piping layout info.

* Instrument engineer:-
  ⇒ Control philosophy, interlock & alarm details, info on shut down and safety features

* Plant engineer or manager
  ⇒ details of utilities & services, existing plant, update on maintenance access & modification.

* Shift operation engineer or supervisor:-
  ⇒ guidance on control instrumentation integrity from an operating view point, info of plant stability at specified control Parameters, info on experienced operability deviations of hazard potential.

* Nodes in HAZOP :-

Nodes Can be :- (lines - Vessels - Plant Sections - Process steps).

- Nodes → Equipment-based nodes. (Typical HAZOP Nodes.)
  → Stream-based nodes (For Flow discussions.)

* Equipment-based nodes :-

- A node is typically limited to one major equipment item and associated Piping, Contol Sys., Safeguarding Sys.

* Stream-based nodes :-

- Based on Stream * Better used in Flow. (Press., temp., level, ...)
- Stream changed along the way
- Stream based nodes solves the tunnel vision Problem & Small nodes.
- it also enable a discussion & operating Procedures, how node start up, Shutdown, operated with equipment out & service.

* objectives of HAZOP analysis :-

- to determine if Process deviation leak to undesirable Consequences.
- to identify operability problems (hazard to personnel, public, Corp. envir.)
- to where more research into Cause & Consequences need to conducted.
- to recommend Changes or improvements to design or operation.

* HAZOP APProch

Process deviation (Parameter + Guide word) → Cause → Consequence → Safeguard. → Action

When Hazop Preformed :- (new Process, modify, Make Changes, Before start up, every 5 years)

* HAZOP Canvas:- (Simples tool.)
- is a Practical way to visual the interworking components of HAZOP.
- it's comprises of eight building blocks.

① Node. ② Deviation. ③ Causes. ④ Consequences.
⑤ Inherent risk ⑥ Safeguards. ⑦ Risk ranking (Operational) ⑧ Recommendations.

* Deviation :- (Slide 94-97)

* Causes :- due to → Equipment Failure
→ Human error.
→ External Factors.

* Consequences:- (Safeguards.

Ex:- (leakage, Dispersion, Fire, Accident, damage, Loss, QC problem)
→ Alternative. (Multiple outcomes of single cause.)
→ unanticipated or unidentified or unmitigated

① SIL : Safety integrity level.
② EIL : Environmental integrity level.
③ CIL : Commercial integrity level.

* Safeguards :-
- Protect integrity of System When deviations may lead to conditions beyond design intentions. → (i.e. Prevention / mitigation)
- types of it :- → Passive / inherently safe
→ Active.
→ Procedural

* Inherently Safe / Passive Safeguard :-
  - Design For max. Press. & Temp.
  - limited Temp. of heating Med.
  - limited inventory used
  - Containment
  - Less Toxic material used.
* Active Safeguards :-
  - Monitoring instrument
  - Alarms
  - interlocks
  - Emergency Relief
  - inert Blanket / Purge
  - Automatic deluge System
* Procedural Safeguards (administration control.)
  - Check lists
  - manual isolation
  - O & M manual / SOP
  - Testing / Analysis

→ identify Plant using P&ID to clarify battery limits & interfaces
→ For existing Plant mean "as built" P&ID
→ For under design use latest revisions of P&ID
→ P&ID use to define Plant with in battery limits

---

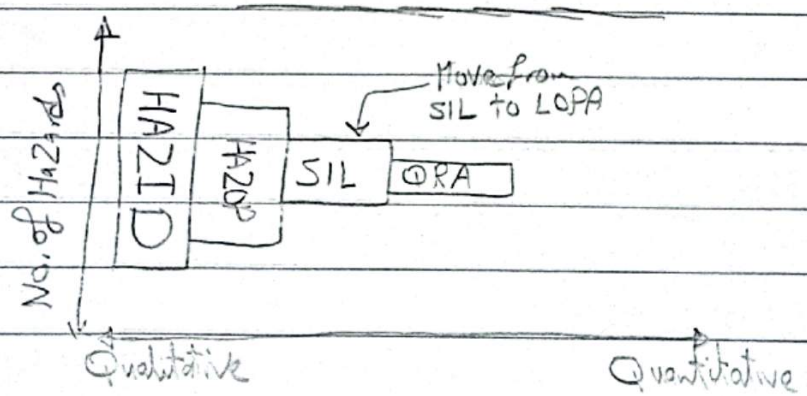
* CHAZOP :- (Control hazard and operability.)
  - Are Part of Safety management Process that Focuses on the potential hazards associated with the operations of the Control System exclusive From the Function of underlying Process
  → it's Focus only the Control and automation System such as (PLCs, DCS, Software, logic, HMI, ...)
  (Program Logic Control)
  - it's not only identify hazards of integrity of the Control System Function but also identify hazards of the operability of Control System
  (Slide 113)
*

* Recommendation :- Can take the form of open or closed action
  - Closed action :-
    - When team agree solution and it's within their Level of Competency. (لما فيش اي حل اقل او اعلى ويمكن اخلص (Closed out form))
  - Open action :-
    - Calling For Further outside HAZOP Study
    - For Cases where Situation is Complex and the Solution is not obvious.

* HAZOP is not :-
  - A Design review (not to catch bad engineering design)
  - A check of the Quality of a design
  - A check of Compliance to Codes and standards
  - A Quantitative risk analysis.
  - An EnA in itself

* Type of Nodes :-
  1. Simple node :- Sample Process
  2. Complex node :- Mode of operation (اكتر من حالة تشغيل)
  3. Global node :- Global effect (اكتر من node بتأثر على بعض)
  4. Super node :- (مجموعة nodes اتعملت Merge مع بعض)

Note :-



* Points to be considered during Re HAZOPs :-
- Plant modifications.
- Changes in operating conditions.
- Different start up / shut down sequences.
- Changes in naming levels / locations.
- Failure to close out actions & Validate their completion
- Degradation of plant integrity or Performance.
- Changes in standards
- New Corporate requirements.
- Plant incidents.
- Increased awareness of due to operating experience.
- Maintenance record.
- Safeguards conditions.
- Documents updates & changes.
- Plant outages & shut down.
- upsets in Process.

* Note HAZOP Co. Make Remote HAZOPing.

what is → * LOPA :- (layer of Protection analysis.)
- Define unwanted impact
- Determine initiating event & Thier frequency.
- Determine conditional modifiers or enabling events.
- " Independent layer of Protection IPL & their PFD.
- Calculate Frequency of impact.

* What need For LOPA :- (HAZOP ومن اين نأتي)
① Hazard Scenario.
② initiating event or initiating causes → (human error & equip. failure) (external factor) ... ومن اين نأتي
③ Consequences. Lead to → THEL (Target mitigated event likehood.)

لو high risk الـ SIL Level كبير & عدد LOPA يزيد THEL (بنختار بيانات)
LOPA اذا كان في فرق كبير بين

④ Safeguard :- ← (IPL) نأخذ

⑤ Recommendation :- لأنها يمكن تصنيف IPL جيد مطلوب.

* PFD ≤ IPL :- لو هيدخل معانا كسبب لـ Failure فصيانة غير و صنعتبر ان 1 يعني مش داخل معانا & 0.1 داخل في الحساب.
يعني اخذ بنة بيك SG ← يزود الخطر لأنه مش شغل SG

* Initiating event Frequency :- يأخذ بعين حسب الـ Stab الشركة المصنعة.

* PFD ≤ IPL :- لو معندناش حاجة بيقي كده (Independent) وهي مستقلة معانا في الحساب وصيانة 1.

* $PFD = \frac{1}{RRF}$

* Ex :- Tank overflow بسبب LCV, human error, $TMEL = 10^{-6}$

		LCV fail	human error	
Basic process control system	IE Freq	0.1	0.2	
integrity safe design	ISD	1	1	← SG هنا التصميم لازم يتعمل
	BPCS	1	0.1	
IPL	Alarm	0.1	0.1	
	PSV	1	1	← Tank لا يوجد فتحة كده فيروح
	Bund	0.1	0.1	
		1×10^{-3}	2×10^{-4}	

$\Rightarrow 1 \times 10^{-3} + 2 \times 10^{-4} \rightarrow 1.2 \times 10^{-3}$

$RRF = \frac{1.2 \times 10^{-3}}{10^{-6}\ (TMEL)} = 1200$

- بناءا على الـ RRF نشوف الـ SIL هقدر اكم وبناءا عليه اعرف المطلوب لـ Valve اتوفير.

* تقسيم الـ SIL : RPF

* SIL (1)	:-	10 —	100
* SIL (2)	:-	100 —	1000
* SIL (3)	:-	1000 —	10000
* SIL (4)	:-	10000 —	100000

---

* ESD :- هتشوف التصميم امن ومحقق الـ SG و X و وبناءا عليه تشوف قيمة الـ LCV Pump اللي هتشتغل بيها 0.1, 0.01
* BPCS :- مثال على Tank فيه LCV & Pump في حالة تعطل الـ Pump دي ممكن يؤثر على الـ Level وممكن يزيد دون توقف فكده الـ RPF بتاعه هتقل 0.1 عن القيمة دي لان الـ Pump اللي فيه عطل الـ LCV بتقاله انه في حالة تعطل الـ LCV فكده لا يوجد اي قيمة تقطيع [1] بالتالي يزود
* Alarm :- حالة عدم وجود alarm يعني RPF بتاعه [1]
* Bund :- نفس مثال الـ BPCS بس التانك دي مكان فيه bund يعني الزيادة اللي هتيجي تنزل على الارض هتقل فيعني RPF بتاعه 0.1

---

* Steps of LOPA :-
  * Step 1 :- Unwanted infact & initiating Cause (hazard scenario & initiating Causes)
  * Step 2 :- Initiating Events (Cause from HAZOP.)
  * Step 3 :- Conditional modifiers (consequences.)
    Ex:- (Probability of ignition, Prob. of exposure, Prob. of injury/fatality, Metrological, Prob. & explosion, time at Risk.)
  * Step 4 :- Identification of IPLS (Safeguard.)
    Ex: (BPCS, Alarms, relief, Document, Human intervention, Machine, hydraulic)
  * Step 5 :- Mitigation (Recombination.)
    Ex: (ESG Syst., Relief device, Flares, Explosive relief, Safety System.)

* Where LOPA may not be appropriate
  1. Low Severity events
  2. Domino events
  3. integrity manegment issues.
  4. Design errors.
  5. Event initiated by external Factors.

* HAZOP TOR :- Terms of reference
* Estimating duration :- Based on ... الوقت المتوقع الذي يستغرق
  - Selection of guide words
  - operating modes.
  - size of nodes
  - size of team
  - experience of leader & team.
  - complexity of site.
  - size of Process.

* HAZOP life Cycle for Project.
  - Coarse HAZOP (what if) (1 week) - Main HAZOP (2-12 weeks)
  - Final HAZOP (2-12 weeks) - Mini HAZOP (1-2 D)
  - ReHAZOP (2-12 weeks)

Note:
- Major equipment (ME)
- Nodes (Nd).
- Total time required for Preparation & organize study (TP) in hour
- " " " " Execute " " (TS) in hour
- " " " " Write the draft report (TW) in hour
- " " to Perform HAZOP study (TH) in hour
- Level Control Valve (LCV)
- Pressure Control Valve (PCV)
- Temperature Control Valve (TCV)
- Flow Control Valve (FCV.)

* Time required for HAZOP.

$$TH = TP + TS + TW + C$$

- TP: Leader + discriper
- TS: Leader + team discriper
- TW: leader + discriper
- C: Constant time related to Preparation & writing = (30-70 h).

* Number of Nodes & time :-
  - Simple : (1-4 Nodes Per PFD) take 1.5 Hr For Preparation & 1.5 Hr Reporting , 2 H line by line
  - Complex : (8-10 Nodes Per PFD) take 1.5 For Pre- & 1.5 For Repot , 5 H
  - Global → 3 H
  - Super node → 4 H

(*) leader & discriper Spend 25% Max time

* Global nodes :-
  - Allow initiating events that effect more than one node
  - issues arise in more than one node

---

* Human error is accepted as Cause in HAZOP Studies (✓)
* Operating Procedure Can take as a Safeguard where is not Practical to engineer an automatic Safeguard.
* Check Valve is not a tight Shut-off device , There Can be Leakage even it in closed Position , Sometimes it's recommed That two dissimilar type of Check Valves install to minimize the reverse flow (not Consider as Safeguard)
* in HAZOP we don't use Fail of last layer of defense to build a scenario which mean we don't Consider Safeguards Such as (PSV , Blowdown Valves , SIS) not taken as Cause
* LOOP in HAZOP means : Called (Control Loop or instrument Loop) . mean set of instruments or Components work together to Control Specific Process Such as Flow , temp , Press , level
* Control Loop Failure Consider as Causes in HAZOP

* The first layer of Protection comes to action is control the Process
* " Second layer of Protection is alarm that get the operator attention to take action. (alarm consider as safeguard)
* Power outage can consider as causes.
* Simultaneous operation of more than required Pumps / Compressors consider as causes
* Fire water System not taken Pump

* Checklist :-
  - is an aide memoire.
  - Check lists can used at any time thought design, existing facility
  - Useful in case of lack of experienced.
  - useful where teams of personnel are not available & individuals are perform.
  - Checklist analysis is an experience-based methodology, codes, standards
  - init operating systems defines inlist of questions. (usually yes/no?)
  - Checklist questions need to develop by multidisciplinary team.
  - Can used at any time to evaluate materials, equipment, procedure,
  - ⇒ it effective combined with a Pre-Start-up safety review)
  - if a hazard analysis conduct at detailed design stage.
  - Can combined with what if for evaluation of hazards.
  - Can used as investigation tool in identify hazards, audit tool in verify designs & installation.
  - ⇒ it's not an aid to identification of unknown hazards.
  - ⇒ Does not identify operability problems well.

* objective of checklist analysis:
  - to verify compliance with design, codes and regulations.
  - to help control MOC.
  - to aid in revised process., aid in training People
  - it's generate from experiences team, from codes, standards,...

* Steps in checklist analysis:
  1. Acquire or develop appropriate check lists
  2. Expert team make tour with leader to compare equipment, operation to checklist items
  3. Deficiencies

* What if Analysis :- (early stage followed by HAZOP & For MOC (غير مفيد))
  - Can used at any time (new or existing).
  - Required on experienced team, creative tea
  - Each question represents Potential Failure or mis operation and focus on specific Consequences such as Process safety, OP, human, environmental ,...
  - Question are applied to existing P&IDs and Process descriptions and usually added as analysis Process.
  - Loose structure.
  - often used at design stage to analyse Proposed changes

* What if Question Areas :-
  - Equipment Failure
  - Human error
  - External events.

* What if Steps :-

1- Provide info to team
2- Leader divides Process to Logical Systems and subsystems
3- Scope & objective of study
4- Existing Safety Precautions
5- Team review info to generate Questions
6- list of Q.
7- Analysis systems & Subsystems to get Q.
8- Potential hazards & Consequences documented
9- Severity & likelihood give risk ranking and documented
10- Recommendation

* HAZOP :-

Process deviation	Causes	Consequences	Safeguard.	Risk Ranking	Recommendation

* What if :- → (left side) (مثلاً HAZOP في ورقة) (right side) في

What If (Failure of Caps)	Consequence	Safeguard	R.R	Recom
ماذا لو حدث Failure في				

* What if + Check list :-

يستخدم (two templet.) في بعض (What if & Check) بعض Mix

* FMEA :- تحليل (equipment list) بعد تحديد risk

= Consequences.

Item/Function	Failure Mode	Failure effect	Safeguard	R.R.	Recom
(Pump, Compressor, Valves ...)	(Rupure, Leakage, Blockage ...)				

* What if / Checklist analysis :-
  - Study start checklist to which what if Q. applied, other study start with Brain storming to identify hazards then checklist.
  - use at any stage & Require expert team.

* objectives of what if / Check list analysis :-
  - identify & evaluate the most common Hazards,
  - Provide Qualitative evaluation of Consequences
  - evaluate the adequacy of existing Safeguard

* FMEA :- (Failure mode and effect analysis.)
  - Analysis specific systems or items of equipment
  - " Mechanical & / or electrical Componets (ex, Pumps, Compressors, ...)
  - Spliting equipments into components then to Sub-Component
  - FMEA Study all Possible Single Failure of individual items and the effect of each failure on item itself and rest of system.
  - FMEA :- is not strictly speaking a hazard identification technique but it Provides an important source of hazard information
  - used at all stages & easily updated For plant modifications.
  - Require equipment Function, Failure modes
  - identified & describes all Possible ways for equipmet to Fail (ex: on/off, open/closed, ...)
  - identified only Single failure modes
  - Not effective in identifying combinations of equipment failures

* FMEA Methodology :-

1- Define the Scope / Function :-
- identified system, equipment, ... to be analyse.

2- Identify Failure mode :-
- list all ways a componet, equi., System could fail

3- Determine effects of each Failure mode :-
- Ass. Consequence of each Failure on System & it's stakeholders
- Evaluate it.

4- Evaluate the Risk :- (RPN بعدين S, O, D نحسب)
- Severity (S) :- impact of Failure (1-10 scale.)
- occurance (O) :- likelihood of Failure (1-10 scale.)
- Detection (D) :- likelihood of detecting the Failure before it reaches the customer (1-10 scale.)
- Risk Priority Number (RPN.) = S x O x D.
- Then Prioritize Failure modes. init Rank Failure modes based on RPN to identify the most Critical risks that need attention (C)

FMECA هي

---

* FMEA :-

- FMECA :(Failure mode and effect Criticality analysis)
(C) بدل (Criticality) بدل (FMEA) هي
(Sheet) في (Column) في (RPN) بدل
بدل

- FMEDA :(Failure mode and effect Diagnosis analysis.)
(Classification) بدل (Diagnosis) بدل (FMEA) هي
Fail (Safe det. (SD), Safe undet. (SU), dangerous det. (DD), dangerous undet. (DU)) بدل (Failure)
Sheet في Column - (Failure Classification) بدل

* Objectives of FMEA :-
  - Provide list of equipmet & Potential Failure.
  - Make evaluate of equi Failure & make Recommendation.

* FMEA :-
  - each Failure mode describe immediate & Surrounding effect
  - Estimate Qualitative S & L → Qualitative risk ranking
  - Describe existing SG & give Recommendation.

* HAZID :- (describe PFD) ...PSID ...
  - it utilizes a matrix of Possible hazard Scenarios against design
  ⇒ - it can used to explore unusual event that might not identified by HAZOP.
  - A Systematic review of Possible Causes & Consequences. (Front-End engineering design.)

* Limitations of PHA :-
  - Can never guarantee identified of all hazards, Causes & Consequences
  - Are only effective if it can safely be assumed that operated in manner intended & according with good practice.
  - Are only relevent to time Conducted.
  - Are Subjective and only as good as knowlege, expert of team.
  - Can only be effective & comprehensive if the info. Complete and accurate and updated.
  - May overlook hazards related to material Quality.
  - Are only effective if action is taken to implement the Recommendation made of study.

- Preparation of PHA report is team leader responsibility
- PHA reports are confidential.
- Worksheet need to be Concise but Complete in detail
- Worksheet & action Sheet are business doc. Can used in Court.
- Do not
  - Do not use expressions that Personal or legal opinions or conclusions
  - Do not judgments about quality of work or Conduct
  - " " words with negative Connotations (ex: Catastrophic, Fatal, ...)
  - " " use words that Constrain management to only one action

* Completed Reports:-
  - Executive Summary of Procedure
  - introduction.
  - Process description
  - Study scope & objectives.
  - Hazard analysis technique.
  - Risk Matrix.
  - Node or System/Subsystem list.
  - Work Sheets
  - Prioritized Recommendation
  - Drawings & other references.

* BOWTIE Analysis :-

- HAZARD :- is a Situation or dormant Potential which could lead to an event When a Cause is activated.
- EVent :- is The moment when control is lost over the hazard, there is no damage or negative impact yet but it's imminent now.
- Cause :- What ever will Lead to an event in Presence of a hazard.
- Barriers :- Will Prevent event occuring in the Presence of the Cause.

---

* What is A barriers :-

Dictionary Definition - Something That blocks or intened to block Passage, (egg) hinder movement or action

Definition by us - A Protective measure Prevent or limit The harm From a major Accident hazards.

* Barrier to Consider Valid it must :-

1- Effective : it Can Prevents Consequences (big enough, fast enough, ...)
2- independant : independant of the initiating event.
3- Available : Can be evaluated to verify it do what should do.

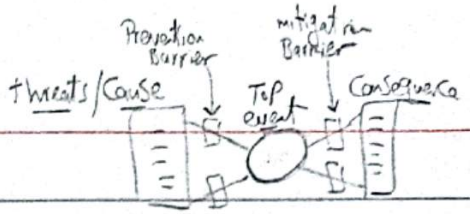
* independent means it has no Common Failure mode (i.e.) amongst other barries on Same Cause or Consequence line

* A Prevention barrier :-

- is described as Fully Functional if it's Capable to Prevent Cause developing into risk event

* A Mitigation barrier :-

- is described as fully Functional if it's Capable of either complete mitigating the Consequence of risk event or reduce Severity



* Bowtie methodology:
  * is used for Risk assessment, Risk management & Risk Communication.
  1. Identify Hazard: (anything from System Crash to event Potential to Cause Significant damage)
     - Top event: is the event that triggers the analysis.
  2. Identify threats: (Causes that could lead to event.) System malfunction to human error
  3. Evaluate Consequences: (Potential Consequ. for the top event.)
  4. Identify barriers: (Prevention or mitigation)
  5. Identify escalation Factors: → (barrier فشل في الأداء أو الكفاءة)
     - Escalation Factors should used sparingly, representing only barrier Failure modes Presenting a major Threat (Preventive or mitigation)

* Steps to describe a barrier:
  - Clear name & Purpose.
  - barrier type & equipment. & Responsible For.

Note: Propane تخزين الضغط في Hazard/Cause (Pressurised Propane Stored in Spheres)

Effectiveness	Condition / State
- it effect - Functionality	- barrier Performing Vs required Performing
- Reliability - availability	- Degradation affects the barrier condition

* Bowties workshops attended by team (Chairman, Scribe, ...).

*PHA leadership:-

- Formal leadership training
- extensive engineering & safety experience.
- Strong ability to interpret eng. drawing

*PHA Quality problems:-

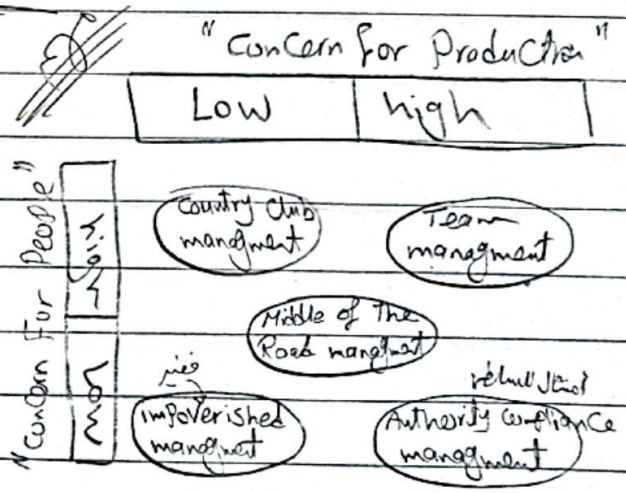
- inappropriate management expectations.
- inadequate time
- Poor scope
- inaccurate data.
- " doc.
- lack & follow up.

* Getting Best of team :- (...)

- Aggressor :- ...
- Dominator :- ...
- Blocker :- ...
- Recognition seeker :-
- Special interest pleader.
- Speed Freak.
- MR. Re-Engineer it.
- joker :-
- Ho Hum Person.

* Leadership styles:-

- To enhance leadership eff.
- it's crucial to develop malleable style integrate various styles
- Two basic management behaviours can be identified as important:-
  1- task oriented behavior.
  2- People oriented behavior



Questions

1- .... The release of a material or energy that has the Potential For Causing harmful effects.

A. Risk
B. Hazard events. (✓)
C. Consequence
D. Accident.

2- During hazard identification, systematic techniques is not recommended as it will affect on group creativity

A. True.
B. False. (✓)
C. Sometimes depend on Process Scope

3- As Per HSE studies the Causes for accident is ...

A. Specifications.
B. maintenance
C. Commissioning.
D. Changes after installations.
E. All of the above (✓)

4- .... The first formal PHA, was developed in UK at ICI over 30 years ago. other methodologies have followed as requirments for Less Comprehensive & time Consuming.

A. what if.
B. LOPA
C. HAZOP (✓)
D. FMEA

5- A PHA assigns qualitative likelihood & severity ratings from which a relative risk ranking Can be estimated

A. True (✓)
B. False.

6- A PHA should be conducted one times only during a Facility's design, before the start-up and introducing the HC to plant.

A. True.
B. False. (✓)

7- The Chance that two (or more) unrelated events or incidents will occur at same time. (it's important to note that two events arising from a common cause do not qualify.)

A- Fail Safe. B- Consequence Failure.

C- Dangerous Failure D- Double Jeopardy (✓)

---

65 - 61 ✗ ✓ element (2) ⇐

1- B. 2- C 3- A 4- B

5- e 6- b

---

121 - 118 ✗ ✓ element (3) ⇐

1- A. 2- E 3- C 4- A, C, F.

---

164 - 162 ✗ element (4) ⇐

1- F. 2- B.

---

266 - 204 ✗ element (6) ⇐

1- A. 2- (D) FMEA 3- B. 4- B

---

220 ✗ element (7) ⇐

1- False